154. CRIPTOGRAFIA COMO DEFESA: PROTEGENDO O DIREITO À PRIVACIDADE

Mayume Caires Moreira
Mestra, Unicesumar.
Maringá – Paraná – Brasil
https://orcid.org/0000-0002-1333-1891
http://lattes.cnpq.br/7810923422029283
mayume.moreira@unicesumar.edu.br

Ellen Fernanda Caselato
Graduanda, Unicesumar.
Maringá – Paraná - Brasil
https://lattes.cnpq.br/6047239214794785
https://orcid.org/0009-0006-4045-2994
caselatoellen@gmail.com

José Paulo Ferreira.
Graduando, Unicesumar.
Maringá – Paraná - Brasil
https://orcid.org/0009-0009-6502-4373
https://lattes.cnpq.br/2859712442904809
jpferreira2023@gmail.com
ra-24000151-2@alunos.unicesumar.edu.br

Leandro Friedrich Querino Pozza.
Graduando, Unicesumar.
Maringá – Paraná - Brasil
http://lattes.cnpq.br/3809224070947391
https://orcid.org/0009-0004-2913-9898
leandropozza1910@gmail.com

RESUMO

Este estudo tem como objetivo investigar a importância da criptografia na proteção da privacidade e no fortalecimento da segurança da informação, especialmente em cenários envolvendo vazamento de dados em redes sociais e processos judiciais. Com o avanço da transformação digital, o uso indevido de dados pessoais tem se tornado uma preocupação crescente. Nesse contexto, a criptografia, como técnica de codificação de informações, surge como uma solução crucial para garantir a confidencialidade e integridade dos dados, evitando acessos não autorizados a informações sensíveis. A pesquisa adota o método indutivo, com base em análises bibliográficas e documentais, visando compreender como a legislação atual protege os cidadãos contra o uso indevido de seus dados e de que forma pode ser aprimorada para lidar com os desafios impostos pela rápida evolução digital. Além disso, o estudo explora os impactos da criptografia no fortalecimento das políticas de proteção de dados, destacando sua contribuição para a segurança cibernética em um ambiente cada vez mais interconectado e vulnerável. A análise também enfoca o papel central da criptografia na construção de políticas públicas mais eficazes para a proteção de dados, com ênfase na prevenção de vazamentos de informações e no combate a crimes cibernéticos. Ao garantir a privacidade e a integridade dos dados pessoais, a criptografia não apenas protege os direitos fundamentais dos indivíduos, mas também fortalece a confiança no ambiente digital, essencial para o funcionamento seguro de sistemas jurídicos, empresariais e sociais.

Palavras chaves: Criptomoedas; Tecnologia; Mídias Sociais.

ABSTRACT

This study aims to investigate the importance of encryption in protecting privacy and strengthening information security, particularly in scenarios involving data leaks on social media and legal proceedings. With the advancement of digital transformation, the misuse of personal data has become an increasing concern. In this context, encryption, as a technique for encoding information, emerges as a crucial solution to ensure the confidentiality and integrity of data, preventing unauthorized access to sensitive information. The research adopts an inductive method, based on bibliographic and documentary analyses, aiming to understand how current legislation protects citizens against the misuse of their data and how it can be improved to address the challenges posed by rapid digital evolution. Furthermore, the study explores the impact of encryption on

strengthening data protection policies, highlighting its contribution to cybersecurity in an increasingly interconnected and vulnerable environment. The analysis also focuses on the central role of encryption in the development of more effective public policies for data protection, emphasizing the prevention of information leaks and the fight against cybercrime. By ensuring the privacy and integrity of personal data, encryption not only protects individuals' fundamental rights but also strengthens trust in the digital environment, which is essential for the secure functioning of legal, business, and social systems.

Keywords: Cryptocurrencies; Technology; Social Media.

1 INTRODUÇÃO

Na sociedade atual, intensamente digitalizada e marcada pela constante troca de informações por meios eletrônicos, a privacidade tornou-se um dos direitos fundamentais mais ameaçados. O avanço das tecnologias da informação, aliado à popularização da internet e das redes sociais, proporcionou uma conectividade sem precedentes, mas também expôs os indivíduos a sérios riscos de violação de seus dados pessoais. Nesse cenário, a segurança da informação e a proteção da privacidade passam a ser temas centrais para o Direito, a tecnologia e a cidadania.

Entre os principais mecanismos para assegurar a proteção dos dados, destaca-se a criptografia. Trata-se de uma tecnologia que codifica informações, tornando-as compreensíveis apenas para aqueles que possuem a chave de acesso apropriada. Essa codificação garante a confidencialidade e a integridade dos dados, sendo uma ferramenta eficaz para evitar acessos não autorizados, roubos de informações e vazamentos que possam comprometer a privacidade dos cidadãos.

O presente estudo tem como objetivo principal analisar a criptografia como uma ferramenta essencial na defesa da privacidade, especialmente no contexto da sociedade digital. Para isso, a pesquisa discute sua aplicação tanto na vida privada quanto no meio jurídico, avaliando como essa tecnologia pode ser implementada de forma eficaz, mesmo diante das limitações técnicas e das exigências legais vigentes. A relevância da temática se justifica pela frequência crescente de casos envolvendo vazamento de dados, ataques cibernéticos e uso indevido de informações pessoais por empresas e instituições governamentais.

Um dos pilares do estudo é a análise da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018 legislação brasileira que regulamenta o tratamento de dados pessoais e estabelece princípios importantes para a segurança da informação. A LGPD reconhece expressamente a necessidade de adoção de medidas técnicas e administrativas para proteger os dados, entre elas, a criptografia. A lei impõe aos controladores e operadores de dados a obrigação de garantir a confidencialidade e a integridade das informações,

prevenindo incidentes que possam prejudicar os titulares dos dados. Nesse sentido, a criptografia torna-se um instrumento legalmente recomendado para assegurar a conformidade com as normas de proteção de dados.

No âmbito judicial, a criptografia também desempenha um papel relevante. Com o avanço da Justiça Digital e a crescente digitalização dos processos judiciais, tornou-se imprescindível garantir a proteção das informações processuais, muitas vezes sigilosas. A criptografia, ao ser aplicada na troca de documentos eletrônicos, petições, provas digitais e até mesmo nas comunicações entre as partes, assegura que apenas os envolvidos tenham acesso ao conteúdo, protegendo o sigilo e a integridade das informações. Esse cuidado é especialmente importante em processos que envolvem dados sensíveis, como casos de família, saúde, menores de idade, entre outros.

A metodologia utilizada neste estudo consiste em uma revisão bibliográfica e documental, com base em obras acadêmicas, legislações nacionais e internacionais, artigos científicos e análises de casos concretos. A pesquisa visa construir uma compreensão crítica e aprofundada sobre os benefícios, os desafios e as limitações da criptografia no contexto jurídico e social atual.

Além dos aspectos técnicos e legais, o estudo também aborda situações reais em que houve violação de privacidade por falta de medidas de segurança adequadas. Casos de grandes vazamentos de dados de usuários em plataformas digitais, ataques hackers a sistemas governamentais e o uso indevido de dados por empresas privadas demonstram a fragilidade da segurança digital quando não há a adoção de ferramentas como a criptografia. Esses episódios evidenciam a necessidade urgente de políticas públicas e estratégias de conscientização da população sobre a importância da proteção de dados.

Por outro lado, é necessário considerar que o uso da criptografia também enfrenta obstáculos, como a resistência de algumas instituições quanto à adoção de tecnologias de segurança, a falta de conhecimento técnico por parte dos usuários e até mesmo conflitos entre o direito à privacidade e a transparência exigida em determinadas situações. Por isso, é fundamental que haja um equilíbrio entre a proteção dos dados pessoais e as demandas legítimas por acesso à informação, especialmente quando envolvem investigações criminais, segurança pública ou interesses coletivos.

Em suma, o estudo propõe uma reflexão crítica sobre a importância da criptografia como aliada na proteção da privacidade no ambiente digital. Ao assegurar que as informações permaneçam acessíveis apenas a quem tem autorização, a criptografia

protege os direitos fundamentais dos cidadãos e contribui para o fortalecimento de uma cultura de segurança cibernética. Sua adoção, tanto no setor público quanto no privado, é indispensável em um mundo onde os dados se tornaram um dos ativos mais valiosos e, ao mesmo tempo, mais vulneráveis.

2 REFERENCIAL TEÓRICO

Este referencial teórico delimita-se em quatro eixos principais: (i) fundamentos técnicos da criptografia e suas modalidades, (ii) bases jurídicas brasileiras e internacionais que recomendam ou exigem o uso da criptografia, (iii) contribuições acadêmicas de autores clássicos e contemporâneos em Direito Digital e Filosofia da Informação, e (iv) aplicações da tecnologia de blockchain no contexto da Justiça Digital. A coleta e análise crítica dessas fontes visam demonstrar como a criptografia sustenta o direito à privacidade e aponta lacunas a serem preenchidas pela investigação.

A criptografia é definida como a ciência que estuda técnicas de codificação de mensagens, com o objetivo de garantir que apenas destinatários autorizados possam compreendê-las. Ela é tradicionalmente dividida em duas categorias principais: criptografia simétrica e criptografia assimétrica. Na criptografia simétrica, a mesma chave é utilizada tanto para a cifragem quanto para a decifragem dos dados, como ocorre nos algoritmos AES (Advanced Encryption Standard) e 3DES (Triple Data Encryption Standard) (EUROPEAN COMMISSION, 2020). Por sua vez, a criptografia assimétrica emprega um par de chaves — uma pública e outra privada —, sendo a base de protocolos como RSA (Rivest-Shamir-Adleman) e ECC (Elliptic Curve Cryptography), os quais também possibilitam a implementação de assinaturas digitais e a troca segura de chaves (EUROPEAN COMMISSION, 2020). Além disso, as funções hash desempenham um papel fundamental na garantia da integridade das mensagens, por meio da geração de resumos criptográficos que permitem identificar qualquer modificação não autorizada nas informações (EUROPEAN COMMISSION, 2020).

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, estabelece como um de seus fundamentos o respeito à privacidade, impondo aos agentes de tratamento a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais. Embora a criptografia não seja mencionada explicitamente na legislação, ela é amplamente reconhecida como uma técnica eficaz para garantir a confidencialidade e a integridade das informações (Gonçalves, 2021).

No contexto europeu, o Parecer 05/2014 do Grupo de Trabalho do Artigo 29 (WP29) qualifica a criptografia como uma forma de pseudonimização, destacando-a entre as principais medidas de segurança a serem adotadas por controladores e operadores de dados (EUROPEAN COMMISSION, 2014). Complementarmente, o Regulamento Geral sobre a Proteção de Dados (GDPR) e documentos técnicos da Autoridade Nacional de Proteção de Dados (ANPD) reforçam que técnicas criptográficas, aliadas a processos de anonimização e pseudonimização, contribuem para mitigar riscos de reidentificação de titulares e para elevar o grau de segurança das bases de dados (Serviços e informações do Brasil, 2022).

No Brasil, Danilo Doneda (ano) foi figura central na elaboração da Lei Geral de Proteção de Dados Pessoais (LGPD), atuando desde a redação inicial até os debates parlamentares que culminaram na sua aprovação. Seu legado é celebrado na obra 5 Anos de LGPD – Estudos em Homenagem a Danilo Doneda (2023), que reúne contribuições acadêmicas sobre a regulação e proteção de dados pessoais no país.

Bruno Ricardo Bioni (ano) destaca que a criptografia transcende o requisito técnico, sendo expressão da autodeterminação informativa e da accountability das organizações, ao assegurar que apenas titulares ou autorizados acessem dados pessoais. Em sua obra Regulação e Proteção de Dados Pessoais (2022), Bioni explora o conceito de accountability como um princípio fundamental na proteção de dados pessoais, enfatizando a responsabilidade das organizações na gestão da informação.

No plano filosófico, Luciano Floridi (2002) defende que a privacidade digital é um componente essencial do direito à informação e da dignidade humana. Em entrevista ao Instituto Humanitas Unisinos (2022), Floridi descreve a criptografia como um “escudo informacional” contra hipervigilância estatal e corporativa, destacando a importância da soberania digital na proteção dos dados pessoais

O whitepaper de Satoshi Nakamoto (2008) introduziu o blockchain como um livro-razão descentralizado e imutável, cuja integridade, ao dispensar intermediários, possibilita o registro seguro de transações e documentos. No contexto judiciário brasileiro, pesquisas recentes exploram o uso da tecnologia blockchain para a preservação de evidências digitais, garantindo uma cadeia de custódia (Chain of Custody) imutável e auditável. Exemplos disso incluem o B-CoC, um sistema baseado em blockchain desenvolvido para garantir a integridade das evidências em perícias forenses, e o modelo computacional proposto por Hélio Silva (2024), que utiliza a tecnologia blockchain para identificação e

coleta de evidências digitais, visando otimizar a cadeia de custódia e assegurar a conformidade com a Lei Geral de Proteção de Dados (LGPD). Adicionalmente, contratos inteligentes (smart contracts) têm o potencial de automatizar atos processuais, proporcionando maior eficiência no sistema judiciário. Contudo, sua implementação plena ainda exige soluções híbridas de arbitragem para a resolução de conflitos, considerando as limitações legais e técnicas da aplicação da tecnologia no direito.

Apesar de a criptografia e o blockchain serem reconhecidos como soluções técnicas robustas, persistem desafios práticos que dificultam sua implementação plena no sistema jurídico brasileiro: Usabilidade: A adoção limitada de ferramentas criptográficas por operadores jurídicos e pelo público geral é atribuída à complexidade técnica dessas soluções, o que representa uma barreira significativa para sua implementação efetiva. Interoperabilidade normativa: Existe uma tensão entre o direito de acesso à informação e a necessidade de garantir a confidencialidade em investigações criminais e de segurança nacional.

A falta de um equilíbrio adequado entre essas duas necessidades compromete a eficácia de soluções baseadas em blockchain no contexto jurídico. Ausência de padronização de protocolos criptográficos: A inexistência de uma padronização unificada de protocolos criptográficos nos sistemas judiciais brasileiros dificulta a realização de auditorias independentes, comprometendo a transparência e a confiança no uso dessas tecnologias. Esta pesquisa visa analisar de forma critica as lacunas mencionadas alinhando à Lei Geral de Proteção de Dados (LGPD) e as práticas internacionais. Além disso, a pesquisa analisará criticamente casos concretos de violação de privacidade para fundamentar recomendações práticas direcionadas a legisladores e gestores de tribunais.

3 METODOLOGIA

A metodologia adotada para a realização deste trabalho é de natureza qualitativa, de cunho exploratório e descritivo, com base em pesquisa bibliográfica e documental. Esse modelo metodológico foi escolhido por permitir uma análise crítica e aprofundada sobre a aplicação da criptografia como ferramenta de proteção da privacidade e dos dados pessoais, tanto no âmbito judicial quanto na vida privada, dentro do contexto da sociedade da informação.

A pesquisa bibliográfica compreendeu o levantamento, a leitura e a análise de livros, artigos acadêmicos, dissertações, teses e publicações científicas que abordam temas

relacionados à criptografia, segurança da informação, privacidade, proteção de dados e Direito Digital. Foram priorizadas obras de autores consagrados na área, como Danilo Doneda, Bruno Bioni, Luciano Floridi e outros estudiosos cujas contribuições são amplamente reconhecidas no campo jurídico e tecnológico.

Além disso, foram incluídas referências técnicas de fontes confiáveis, como relatórios da Agência Nacional de Proteção de Dados (ANPD), publicações internacionais da União Europeia e normativas do GDPR. A pesquisa documental, por sua vez, concentrou-se na análise de legislações, diretrizes técnicas e normativas que regem a proteção de dados e o uso de tecnologias de segurança da informação. Dentre os principais documentos examinados estão a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), o Marco Civil da Internet (Lei n.º 12.965/2014), o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), além de pareceres e notas técnicas emitidas por órgãos reguladores nacionais e internacionais.

O objetivo foi compreender como a criptografia é tratada juridicamente e quais exigências legais se aplicam ao seu uso como mecanismo de proteção à privacidade. A abordagem utilizada foi predominantemente dedutiva, partindo de conceitos gerais sobre privacidade e segurança digital até alcançar o objeto específico da pesquisa, que é a análise da criptografia como instrumento de defesa dos direitos fundamentais em ambientes digitais.

Além disso, foram selecionados e discutidos estudos de caso que ilustram situações concretas de vazamento de dados, falhas de segurança e aplicação (ou ausência) de criptografia em processos judiciais e comunicações privadas. A análise dos dados obtidos foi feita por meio de uma interpretação crítica e comparativa do conteúdo das fontes selecionadas, buscando identificar convergências, divergências, lacunas e oportunidades de aprimoramento no uso da criptografia como mecanismo de proteção. A proposta não é quantificar dados, mas compreender o fenômeno de forma contextualizada, interdisciplinar e coerente com os objetivos da pesquisa. Com esse conjunto metodológico, espera-se oferecer uma base sólida para sustentar as reflexões propostas no trabalho e contribuir para o debate acadêmico e jurídico sobre os desafios e as potencialidades da criptografia na era da informação.

4 RESULTADOS ESPERADOS

A presente pesquisa, ainda em fase de desenvolvimento final, já permite identificar resultados relevantes no que se refere à compreensão do papel da criptografia como mecanismo de proteção à privacidade e aos dados pessoais na era digital. A partir da análise bibliográfica e documental realizada, bem como do exame crítico das legislações e casos concretos selecionados, foi possível destacar contribuições importantes e estabelecer diretrizes que fundamentam os resultados esperados.

Em primeiro lugar, observou-se que a criptografia é amplamente reconhecida na doutrina e na legislação como um método eficaz de proteção de dados sensíveis, tanto no setor privado quanto no âmbito público. Os dados obtidos demonstram que a utilização da criptografia permite mitigar riscos relacionados ao vazamento de informações, acessos não autorizados e exposição indevida de dados pessoais, principalmente em sistemas conectados à internet. Este reconhecimento é reforçado por marcos legais como a Lei Geral de Proteção de Dados (LGPD), que menciona expressamente a adoção de medidas técnicas como a criptografia para garantir a segurança e a integridade das informações tratadas.

Além disso, os estudos de caso levantados durante a pesquisa evidenciam que a ausência de criptografia ou sua implementação inadequada está diretamente relacionada a violações significativas de privacidade, como ocorreu em diversos episódios de vazamentos massivos de dados. Tais casos reforçam a urgência da implementação de políticas de segurança da informação eficazes, que incluam não apenas a adoção da criptografia, mas também treinamentos, auditorias e governança de dados adequadas.

Desse modo, espera-se com este estudo demonstrar a viabilidade da criptografia em ambientes judiciais, sobretudo diante da digitalização crescente de processos e da adoção da Justiça 4.0. O uso de assinaturas digitais e certificados criptográficos em petições, laudos e comunicações entre advogados, partes e magistrados vem se consolidando como uma prática segura e alinhada com os princípios constitucionais da legalidade, publicidade e proteção dos direitos fundamentais. A tendência é que esses mecanismos se tornem cada vez mais indispensáveis em processos judiciais eletrônicos, sobretudo na proteção de dados de vítimas, testemunhas e menores.

Espera-se também que a pesquisa contribua para reforçar a percepção da criptografia como um direito digital, inserido no contexto dos direitos fundamentais à privacidade e à autodeterminação informativa. A partir da revisão teórica conduzida, nota-se um consenso crescente entre os estudiosos do Direito Digital de que a criptografia deve

ser tratada não apenas como ferramenta técnica, mas como elemento essencial da proteção da dignidade da pessoa humana na sociedade da informação. Por fim, o estudo pretende ainda colaborar para o debate sobre os limites e desafios da criptografia, especialmente quando confrontada com princípios como a transparência governamental, o acesso à informação e o dever de colaboração com autoridades públicas. A conciliação entre segurança da informação e direitos coletivos será um dos temas centrais nos resultados finais da pesquisa.

REFERÊNCIAS UTILIZADAS

SBAITE GONÇALVES, Mariana. A LGPD não faz referência à criptografia?. Consultor Jurídico, 21 maio 2021. Disponível em: https://www.conjur.com.br/2021-mai-21/opiniao-lgpd-nao-faz-referencia-criptografia/ Acesso em: 19 mai. 2025.

SERVIÇOS E INFORMAÇÕES DO BRASIL. Estudo Técnico sobre Anonimização na LGPD. Autoridade Nacional de Proteção de Dados – ANPD, 2022. Acesso em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes Acesso em: 19 mai. 2025.

BIONI, Bruno Ricardo. Regulação e Proteção de Dados Pessoais. 2022. Disponível em: https://brunobioni.com.br/livros/regulacao-e-protecao-de-dados-pessoais/ Acesso em: 19 mai. 2025.

DONEDA, Danilo. 5 Anos de LGPD – Estudos em Homenagem a Danilo Doneda. 2023. Disponível em: https://doneda.net/2023/11/26/lancamento-do-livro-5-anos-de-lgpd-estudos-em-homenagem-a-danilo-doneda. Acesso em: 19 mai. 2025.

FLORIDI, Luciano. "Os Estados devem retomar a soberania digital." Entrevista concedida ao Instituto Humanitas Unisinos. 2022. Acesso em: https://www.ihu.unisinos.br/publicacoes/78-noticias/606178-os-estados-devem-retomar-a-soberania-digital-entrevista-com-luciano-floridi Acesso em: 19 mai. 2025.

HÉLIO SILVA, Fabian Andrade. Modelo computacional para cadeia de custódia digital: identificação e coleta com base em tecnologia blockchain. 2024. Dissertação (Mestrado em Computação Aplicada) – Universidade Tecnológica Federal do Paraná, Curitiba, 2024. Acesso em: https://repositorio.utfpr.edu.br/jspui/handle/1/34603 Acesso em: 19 mai. 2025.

BONOMI, Silvia; CASINI, Marco; CICOTELLI, Claudio. B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics. arXiv, 2018. Acesso em: https://arxiv.org/abs/1807.10359 Acesso em: 19 mai. 2025.

ASSIS, Gabriel. O uso do blockchain como ferramenta na preservação de provas digitais. Revista FT, [S.l.], v. 1, n. 1, p. 1-10, 2022. Acesso em: https://revistaft.com.br/o-uso-do-blockchain-como-ferramenta-na-preservacao-de-provas-digitais Acesso em: 19 mai. 2025.

MOTTA, Naiara; LOPES, Joathan; ALVES, Marcela; KURIBAYASHI, Hugo Pereira. Uma perspectiva tecnológica para o uso de Blockchain na Identificação Civil: uma revisão

sistemática. Revista Brasileira de Computação Aplicada, [S.l.], v. 16, n. 1, p. 1-15, 2024. Acesso em: https://seer.upf.br/index.php/rbca/article/view/15113 Acesso em: 19 mai. 2025.

SASAKI, Elton. Modelo de utilização de tecnologia blockchain no sistema registral e notarial brasileiro. 2018. Dissertação (Mestrado em Direito) – Universidade Federal do Paraná, Curitiba, 2018. Acesso em: https://acervodigital.ufpr.br/xmlui/handle/1884/92154 Acesso em: 19 mai. 2025.